

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-374244

(43)Date of publication of application : 26.12.2002

(51)Int.Cl.

H04L 9/32

G10K 15/02

G10L 19/00

G11B 20/10

(21)Application number : 2001-179240

(71)Applicant : KENWOOD CORP

(22)Date of filing : 13.06.2001

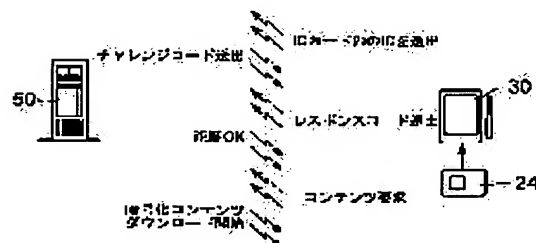
(72)Inventor : ISHIDA MASARU

(54) INFORMATION DISTRIBUTION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information distribution method, by which many unspecified terminals can download and reproduce contents, transfer the downloaded contents to other device or record the downloaded contents to other recording medium for reproduction by the other device, a diversified recording media can be used and unauthorized use of contents can be prevented fully.

SOLUTION: This method employs an IC card 24, that records an ID by each user to identify a user and a secret key by each user used, for identifying the user and for encrypting/decrypting data. A mobile phone 30, to which the IC card 24 is loaded, is connected to a server 50 via a communication line, and the server 50 authenticates the user by using the ID and the secret key in the IC card 24. When the server 50 authenticates the user, the server 50 distributes encrypted contents, by using the same secret key as that in the IC card 24 to the mobile phone 30. The distributed contents are decrypted and reproduced, by using the secret key in the IC card 24.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-374244
(P2002-374244A)

(43) 公開日 平成14年12月26日 (2002. 12. 26)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/32		G 1 0 K 15/02	5 D 0 4 4
G 1 0 K 15/02		G 1 1 B 20/10	H 5 J 1 0 4
G 1 0 L 19/00		H 0 4 L 9/00	6 7 5 A
G 1 1 B 20/10		G 1 0 L 9/00	N
		H 0 4 L 9/00	6 7 3 E
審査請求 未請求 請求項の数 6 O L (全 6 頁)			

(21) 出願番号 特願2001-179240 (P2001-179240)

(22) 出願日 平成13年6月13日 (2001. 6. 13)

(71) 出願人 000003595

株式会社ケンウッド

東京都八王子市石川町2967番地3

(72) 発明者 石田 勝

東京都渋谷区道玄坂1丁目14番6号 株式
会社ケンウッド内

(74) 代理人 100086368

弁理士 萩原 誠

Fターム(参考) 5D044 AB05 AB07 BC04 CC06 DE50

GK12 GK17 HL08

5J104 AA07 AA12 KA01 KA06 NA02

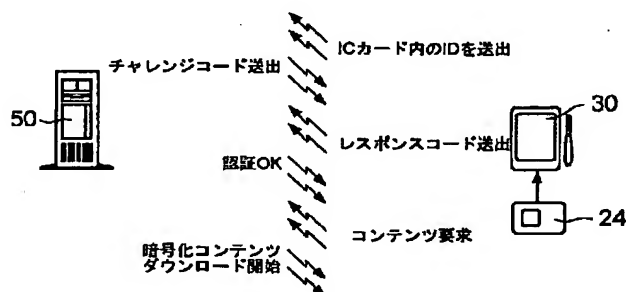
NA35 NA36 NA37 NA41 PA02

(54) 【発明の名称】 情報配信方法

(57) 【要約】

【課題】 不特定多数の端末でコンテンツをダウンロードし再生することができ、ダウンロードされたコンテンツは他の機器に転送して、或いは他の記録媒体に記録して他の機器で再生することもでき、記録媒体は様々な記録媒体を利用でき、コンテンツの不正使用防止も充分図れる情報配信方法を提供すること。

【解決手段】 ユーザを特定するためのユーザ毎のIDとユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録したICカード24を使用する。このICカード24を装填した移動体電話機30を通信回線を介してサーバ50と接続して、ICカード24内のIDと秘密鍵を使用してユーザの認証をサーバ50で得る。認証が得られると、ICカード24内の秘密鍵と同一秘密鍵で暗号化されたコンテンツをサーバ50より移動体電話機30に配信する。配信されたコンテンツはICカード24内の秘密鍵を使用して復号化して再生される。



【特許請求の範囲】

【請求項 1】 ユーザを特定するためのユーザ毎の ID とユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録した情報カードと、この情報カードを有する端末を通信回線を介してサーバと接続して、前記情報カード内の ID と秘密鍵を使用してユーザの認証をサーバ側で得る手段と、この手段で認証が得られると、前記情報カード内の秘密鍵と同一秘密鍵で暗号化された情報を前記サーバより前記端末に配信し、端末の記録媒体に情報を格納する手段とを具備することを特徴とする情報配信方法。

【請求項 2】 配信された前記情報を前記情報カード内の秘密鍵を使用して復号化して再生する手段が付加されたことを特徴とする請求項 1 に記載の情報配信方法。

【請求項 3】 前記再生は、情報が配信された前記端末で行われることを特徴とする請求項 2 に記載の情報配信方法。

【請求項 4】 前記再生は、端末に配信された情報を他の機器に転送して、あるいは他の記録媒体に記録して他の機器で行われることを特徴とする請求項 2 に記載の情報配信方法。

【請求項 5】 前記情報カード内の前記 ID および前記秘密鍵は暗号化されていることを特徴とする請求項 1 ないし 4 のいずれかに記載の情報配信方法。

【請求項 6】 前記認証は、第 1 に端末から情報カード内の ID をサーバに送出し、第 2 にサーバからチャレンジコードを端末に送出し、第 3 に端末から情報カード内の秘密鍵を使用して生成されたレスポンスコードをサーバに送出することにより行われることを特徴とする請求項 1 ないし 5 のいずれかに記載の情報配信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報配信方法に関する。

【0002】

【従来の技術】最近、パソコンや移動体電話機、あるいは携帯プレーヤなどの端末に対して通信回線を介して音楽などの情報を配信するサービスが数多く行われている。

【0003】図 6 は、従来の情報配信方法を移動体電話機を例にとって説明するための図である。この図において、11 は移動体電話機、12 は配信サーバである。情報の配信を行う場合は、まず移動体電話機 11 において発信動作が行われ、移動体電話機 11 が通信回線を介して配信サーバ 12 に接続される。すると、移動体電話機 11 から端末固有の情報、例えば内部に保存されている自機の電話番号がサーバ 12 に送出される。サーバ 12 は、この電話番号を受信して、端末（移動体電話機 11）が情報（以下コンテンツと言う）を利用できる端末であるか否かを判断する。そして、サーバ 12 において

移動体電話機 11 がコンテンツを利用できる端末であると確認されると、サーバ 12 は、移動体電話機 11 に対してパスワードを要求する。この要求に対して移動体電話機 11 はパスワードをサーバ 12 に送出する。そして、このパスワードが正しいとサーバ 12 で判断されると、サーバ 12 は認証 OK を移動体電話機 11 に通知する。すると、移動体電話機 11 はコンテンツの要求をサーバ 12 に送出し、サーバ 12 はその要求を受けてコンテンツのダウンロード（配信）を開始する。ダウンロードされたコンテンツは、移動体電話機 11 内の記録媒体に格納され、移動体電話機 11 で再生できる。

【0004】

【発明が解決しようとする課題】このように、従来は、電話番号など、端末内部に直接保存されている情報を使用して、端末がコンテンツを利用できる端末であることを確認して、その端末に限ってコンテンツをダウンロードしている。したがって、同一ユーザでも端末を変えてコンテンツをダウンロードできないし、ダウンロードされたコンテンツを端末から他の機器に転送させることもできなかった。図 7 は転送の様子を示しており、コンテンツがダウンロードされた移動体電話機 11 からパソコン 13 にコンテンツを転送して CD-R（追記型光ディスク）14 にコンテンツを書込もうとしているが、従来は不可能であった。また、従来は、ダウンロードされたコンテンツを格納する記録媒体に著作権保護機構を付ける必要があるから、利用できる記録媒体の種類が限られていた。

【0005】本発明は上記の点に鑑みなされたもので、その目的は、不特定多数の端末でコンテンツをダウンロードし再生することができるとともに、ダウンロードされたコンテンツを他の機器に転送して、あるいは他の記録媒体に記録して他の機器で再生することもでき、さらには、コンテンツを格納する記録媒体として様々な記録媒体を利用できるとともに、コンテンツの不正使用を充分防止できる情報配信方法を提供することにある。

【0006】

【課題を解決するための手段】本発明の情報配信方法は、ユーザを特定するためのユーザ毎の ID とユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録した情報カードと、この情報カードを有する端末を通信回線を介してサーバと接続して、前記情報カード内の ID と秘密鍵を使用してユーザの認証をサーバ側で得る手段と、この手段で認証が得られると、前記情報カード内の秘密鍵と同一秘密鍵で暗号化された情報を前記サーバより前記端末に配信し、端末の記録媒体に情報を格納する手段とを具備することを特徴とする。

【0007】好ましい形態として、配信された前記情報を前記情報カード内の秘密鍵を使用して復号化して再生する手段が付加される。この手段による再生は、情報が配信された前記端末で行われる。あるいは、端末に配信

された情報を他の機器に転送して、あるいは他の記録媒体に記録して他の機器で再生が行われる。前記情報カード内の前記 ID および前記秘密鍵は暗号化されている。また、前記認証は、第 1 に端末から情報カード内の ID をサーバに送出し、第 2 にサーバからチャレンジコードを端末に送出し、第 3 に端末から情報カード内の秘密鍵を使用して生成されたレスポンスコードをサーバに送出することにより行われる。

【0008】

【発明の実施の形態】次に添付図面を参照して本発明による情報配信方法の実施の形態を詳細に説明する。本発明の実施の形態では、ユーザを特定するためのユーザ毎の ID と、ユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録した情報カードが使用される。この情報カードとしては具体的には IC カードが使用される。IC カードへの ID および秘密鍵の書き込みは、配信業者にて行われる。ID および秘密鍵は、情報の外部漏洩を防止するため暗号化されて IC カード内に記録される。

【0009】図 3 は、IC カードへの ID および秘密鍵の書き込み方法を具体的に示す図である。この図において、21 はパソコン、22 はマスタ鍵保管装置、23 は IC カードリーダライタである。マスタ鍵保管装置 22 は、マスタ鍵を保管し、各ユーザの秘密鍵を生成するときに参照される。IC カードリーダライタ 23 は、IC カード 24 のデータの読込み、書き込みを行う。パソコン 21 は IC カード書き込み専用ソフトウェアを有し、ID の設定、秘密鍵の生成、マスタ鍵保管装置 22 および IC カードリーダライタ 23 の制御を行う。

【0010】上記装置によって IC カード 24 へ ID および秘密鍵を書込む場合は、まずパソコン 21 にマスタ鍵保管装置 22 と IC カードリーダライタ 23 を接続し、電源を入れる。次に、パソコン 21 を起動し、IC カード書き込み専用ソフトウェアを起動する。次に、書き込み処理初回時のみ、パソコン 21 において、マスタ鍵保管装置 22 内の使用するマスタ鍵を設定する。次に、パソコン 21 において、IC カード書き込み専用ソフトウェアの画面に ID を設定する。その後、IC カード 24 を IC カードリーダライタ 23 に挿入する。その後、パソコン 21 において、IC カード書き込み専用ソフトウェアに書き込み指示をする。すると、パソコン 21 の IC カード書き込み専用ソフトウェアの画面に設定された ID が IC カードリーダライタ 23 によって IC カード 24 に書き込まれるとともに、マスタ鍵保管装置 22 内のマスタ鍵を使用してパソコン 21 で生成された秘密鍵が IC カードリーダライタ 23 によって IC カード 24 に書き込まれる。このとき、ID および秘密鍵は暗号化されて IC カード 24 に書き込まれる。

【0011】図 4 は、本発明の実施の形態でダウンロード端末として使用されるオーディオ再生機能付き移動体

電話機 30 の構成を示すブロック図である。この移動体電話機 30 は、通信機能部 31、表示部 32、入力部 33、CPU 34、IC カード読取り部 35、メモリ 36、デコーダ部 37、アンプ部 38、およびインタフェース部 39 で構成される。

【0012】通信機能部 31 は、移動体電話機の通信部分で、基地局と通信を行う。表示部 32 は、電話番号やコンテンツ情報などを表示する。入力部 33 は、電話番号やコンテンツの指示などの情報を入力する。CPU 34 は、電話機の制御全般を行う。IC カード読取り部 35 は、図 3 の IC カード 24 に記録されている ID および秘密鍵を読取る。メモリ 36 は、ダウンロードしたデータ（コンテンツ）を格納する。デコーダ部 37 は、IC カード読取り部 35 で読取られた図 3 の IC カード 24 内の秘密鍵を使用してメモリ 36 内のデータ（コンテンツ）を復号化する。アンプ部 38 は、復号化された信号を、ヘッドホンを駆動するために増幅する。このアンプ部 38 の出力にヘッドホン 40 が接続される。インタフェース部 39 は、電話機をパソコンなどと接続するためのインタフェースである。

【0013】本発明の実施の形態では、図 1 に示すように、ユーザ毎の ID と秘密鍵とが図 3 の装置で書き込まれた IC カード 24 を図 4 の移動体電話機 30 に装填して、前記 IC カード 24 内の ID および秘密鍵を使用してユーザの認証を配信サーバ 50 側で行いながら、前記秘密鍵と同一秘密鍵で暗号化されたコンテンツが配信サーバ 50 から移動体電話機 30 に対してダウンロードされる。このダウンロードの詳細を前記図 1 と図 2 のフローチャートを参照して以下説明する。

【0014】ダウンロードを開始する場合は、まず移動体電話機 30 で発信動作が行われる。この発信動作により移動体電話機 30 は通信回線に接続され（ステップ S1）、さらに通信回線を介して配信サーバ 50 に接続される（ステップ S2）。すると、移動体電話機 30 は、装填された IC カード 24 から ID を読取って（ステップ S3）、ID をサーバ 50 に送出する（ステップ S4）。サーバ 50 は、送出された ID を受信して、受信した ID によりユーザを確認し、そのユーザに対する固有のチャレンジコードを生成して、そのチャレンジコードを移動体電話機 30 に送出する。

【0015】移動体電話機 30 は、チャレンジコードを受信すると（ステップ S5）、そのチャレンジコードに対して、IC カード 24 内の秘密鍵を使用してレスポンスコードを生成し（ステップ S6）、そのレスポンスコードをサーバ 50 に送出する（ステップ S7）。サーバ 50 は、送出されたレスポンスコードを受信して、受信したレスポンスコードが正しいか判断し、正しければ認証 OK を移動体電話機 30 に通知し（ステップ S8）、動作を継続する。ここで、認証が OK でなかった場合は、サーバ 50 は通信回線を切断し（ステップ S1

1)、動作を終了する。

【0016】認証がOKとなると(ステップS8)、移動体電話機30はサーバ50に対してコンテンツの要求を送出する(ステップS9)。サーバ50は、その要求を受信すると、ICカード24に記録されている秘密鍵と同一の秘密鍵(現在のユーザの秘密鍵でサーバ50内に保管されている)でコンテンツを暗号化して該コンテンツを移動体電話機30にダウンロードする。すると、移動体電話機30は、ダウンロードされた暗号化されたコンテンツを受信し(ステップS10)、電話機内の図4のメモリ36に格納する。そして、コンテンツを全て受信し終わると、移動体電話機30は通信回線を切断し(ステップS11)、動作を終了する。

【0017】その後、図4のメモリ36に格納されたコンテンツを読出して、ICカード24内の秘密鍵を使用して図4のデコーダ部37でコンテンツを復号化することにより、移動体電話機30のヘッドホン40でコンテンツを再生できる。

【0018】このように、上記の方法によれば、ICカード24内のIDおよび秘密鍵によりユーザの認証を行う。したがって、このICカード24を端末に対して着脱自在として多数の端末で使うことができるようにすることにより、不特定多数の端末でコンテンツをダウンロードすることができ、利便性が向上する。また、ダウンロードされたコンテンツはICカード24内の秘密鍵で復号化してダウンロードされた端末で再生することができるが、さらには他の機器に転送して、あるいは他の記録媒体に記録して他の機器でICカード24を使用して再生することができ、利用範囲を広げることができる。

【0019】図5は、他の機器でコンテンツを再生する場合の具体例を示す。この具体例は、移動体電話機30にダウンロードしたコンテンツをパソコン61に転送してパソコン61でCD-R62に書き込み、このCD-R62を使用してカーオーディオ機器63でコンテンツを再生する場合である。その場合は、まず、ICカード24を移動体電話機30に装填してコンテンツを移動体電話機30にダウンロードさせる。次に、ダウンロードしたコンテンツを移動体電話機30からUSB経由でパソコン61に転送する。次いで、転送したコンテンツをパソコン61でCD-Rドライブを使用してCD-R62に書き込む。その後、CD-R62とICカード24をカーオーディオ機器63に移し、ICカード24内の秘密鍵でCD-R62内のコンテンツを復号化しながらカー

オーディオ機器63でコンテンツを再生する。

【0020】このとき、ICカード24が無ければコンテンツの復号化および再生ができないため、上記のように他の記録媒体にコンテンツを書込んだり、他の機器にコンテンツを転送しても、本発明の方法によれば、コンテンツの不正使用は充分防止できる。また、コンテンツ自体が暗号化されていて、記録媒体でコンテンツの保護を図る必要がないので、本発明の方法によれば、移動体電話機内の半導体メモリやCD-Rなど様々な記録媒体を利用できる。

【0021】なお、コンテンツは、転送先の機器、図5ではパソコン61でICカード24を使用して再生することもできる。また、ダウンロードし再生するコンテンツは、音楽情報や画像情報、あるいは案内情報などのどれでもよく、種類を問わない。さらに、コンテンツをダウンロードする端末も移動体電話機に限定されない。

【0022】

【発明の効果】以上詳細に説明したように本発明の情報配信方法によれば、不特定多数の端末でコンテンツをダウンロードし再生することができるとともに、ダウンロードされたコンテンツを他の機器に転送して、あるいは他の記録媒体に記録して他の機器で再生することもでき、さらには、コンテンツを格納する記録媒体として様々な記録媒体を利用できるとともに、コンテンツの不正使用を充分防止できる。

【図面の簡単な説明】

【図1】本発明による情報配信方法の実施の形態を説明するための図。

【図2】本発明による情報配信方法の実施の形態を示すフローチャート。

【図3】ICカードへのIDおよび秘密鍵の書き込み方法を具体的に示す図。

【図4】本発明の実施の形態でダウンロード端末として使用されるオーディオ再生機能付き移動体電話機の構成を示すブロック図。

【図5】ダウンロードされたコンテンツを他の機器で再生する場合の具体例を示す図。

【図6】従来の情報配信方法を移動体電話機を例にとつて説明するための図。

【図7】従来技術の問題点を説明するための図。

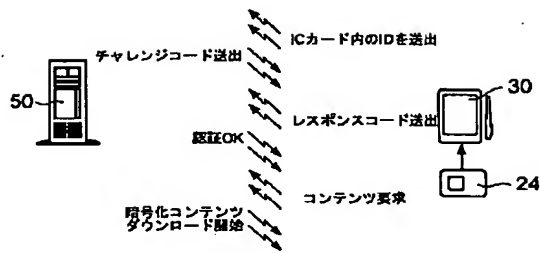
【符号の説明】

24 ICカード

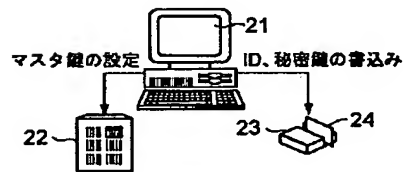
30 移動体電話機

50 サーバ

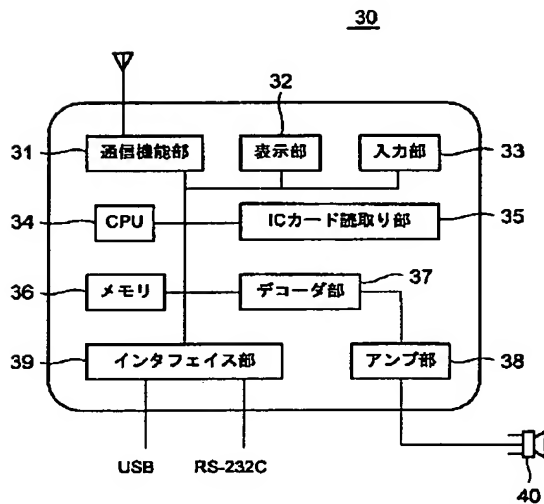
【図 1】



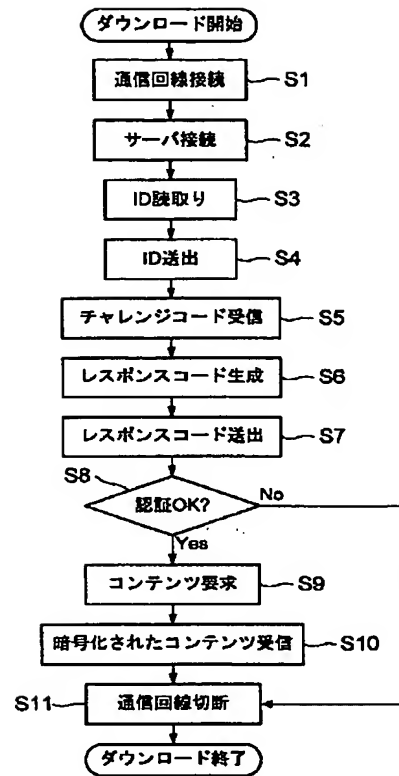
【図 3】



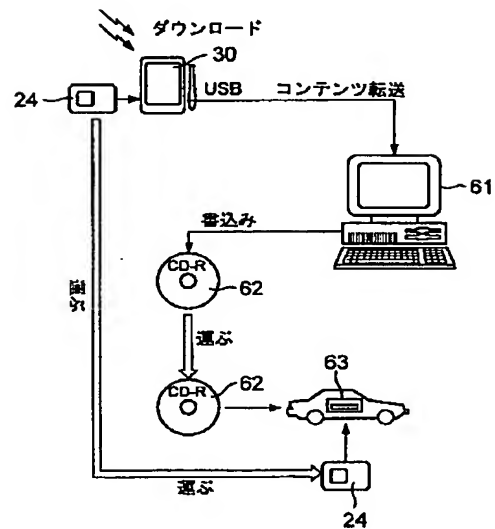
【図 4】



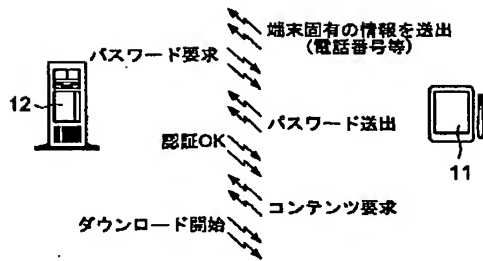
【図 2】



【図 5】



【図6】



【図7】

